

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF TEXAS
WACO DIVISION**

PACSEC3, LLC,)	
Plaintiff,)	
)	Civil Action No. 6:22-cv-00126
v.)	
)	
DARKTRACE, PLC,)	JURY TRIAL DEMANDED
Defendant.)	

PLAINTIFF’S ORIGINAL COMPLAINT FOR PATENT INFRINGEMENT

PacSec3, LLC (“PacSec”) files this Original Complaint and demand for jury trial seeking relief from patent infringement of the claims of U.S. Patent No. 7,523,497 (“the ‘497 patent”) (referred to as the “Patent-in-Suit”) by Darktrace, plc (“Darktrace”).

I. THE PARTIES

1. Plaintiff PacSec3, LLC is a Texas Limited Liability Company with its principal place of business located in Harris County, Texas.

2. On information and belief, Darktrace is a corporation organized under the laws of the England and Wales with a regular and established place of business at 501 Congress Ave., Suite 150, Austin, TX 78701. On information and belief, DARKTRACE sells and offers to sell products and services throughout Texas, including in this judicial district, and introduces products and services that perform infringing methods or processes into the stream of commerce knowing that they would be sold in Texas and this judicial district. DARKTRACE can be served with process through their place of business or wherever they may be found.

II. JURISDICTION AND VENUE

3. This Court has original subject-matter jurisdiction over the entire action pursuant to 28 U.S.C. §§ 1331 and 1338(a) because Plaintiff's claim arises under an Act of Congress relating to Patent, namely, 35 U.S.C. § 271.

4. This Court has personal jurisdiction over Defendant because: (i) Defendant is present within or has minimum contacts within the State of Texas and this judicial district; (ii) Defendant has purposefully availed itself of the privileges of conducting business in the State of Texas and in this judicial district; and (iii) Plaintiff's cause of action arises directly from Defendant's business contacts and other activities in the State of Texas and in this judicial district.

5. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 1400(b). Defendant has committed acts of infringement and has a regular and established place of business in this District. Further, venue is proper because Defendant conducts substantial business in this forum, directly or through intermediaries, including: (i) at least a portion of the infringements alleged herein; and (ii) regularly doing or soliciting business, engaging in other persistent courses of conduct and/or deriving substantial revenue from goods and services provided to individuals in Texas and this District.

III. INFRINGEMENT OF THE '497 PATNET

6. On April 21, 2009, U.S. Patent No. 7,523,497 ("the '497 patent", included as an attachment) entitled "PACKET FLOODING DEFENSE SYSTEM," was duly and legally issued by the U.S. Patent and Trademark Office. PacSec3, LLC owns the '497 patent by assignment.


7. The '497 patent relates to a novel and improved manner and system of defense to a data packet flood attack.

8. DARKTRACE offers for sale, sells and manufactures one or more firewall systems that infringes one or more claims of the '497 patent, including one or more of claims 1-18, literally or

under the doctrine of equivalents. Defendant put the inventions claimed by the ‘497 Patent into service (i.e., used them); but for Defendant’s actions, the claimed-inventions embodiments involving Defendant’s products and services would never have been put into service. Defendant’s acts complained of herein caused those claimed-invention embodiments as a whole to perform, and Defendant’s procurement of monetary and commercial benefit from it.

9. Support for the allegations of infringement may be found in the following preliminary table:

10.

US7523497 B2 Claim 7	Darktrace
7. A method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets, said method comprising the steps of:	 A screenshot of the Darktrace website. The background is dark blue with a network-like pattern of glowing blue lines and nodes. In the top left corner is the Darktrace logo, which consists of a stylized orange and white icon followed by the word "DARKTRACE" in white capital letters. In the top right corner, there is a white button with the text "Free Trial" and a white hamburger menu icon. The main heading in the center reads "World leaders in Autonomous Cyber AI" in a large, white, serif font. Below the heading, there is a paragraph of white text: "Darktrace AI interrupts in-progress cyber-attacks in seconds, including ransomware, email phishing, and threats to cloud environments and critical infrastructure. Join over 6,500 organizations worldwide that rely on a digital immune system to avoid cyber disruptions, without impacting regular business operations."

© 2022, Darktrace

<<https://www.darktrace.com/en/>>

Darktrace has a method of providing packet flooding defense for a network comprising a plurality of host computers, routers, communication lines and transmitted data packets.

The reference includes subject matter disclosed by the claims of the patent after the priority date.

The venue of the company is:

501 Congress Avenue

Suite 150

Austin, TX 78701

United States

US7523497 B2
Claim 7

Darktrace

determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer;

A major challenge in modeling the behaviors of a dynamically evolving infrastructure is the huge number of potential predictor variables. For the observation of packet traffic and host activity within an enterprise LAN or WAN, where both input and output can contain many inter related features (protocols, source and destination machines, log changes, and rule triggers), learning a sparse and consistent structured predictive function is crucial.

In this context, Darktrace employs a, cutting-edge large- scale computational approach to understand sparse structure in models of network connectivity based on applying L1- regularization techniques (the lasso method). This allows Darktrace's AI to discover true associations between different elements of a network which can be cast as efficiently solvable convex optimization problems and yield parsimonious models.

<<https://www.darktrace.com/en/resources/wp-machine-learning.pdf>>

The reference describes determining a path by which data packets arrive at a host computer via packet marks provided by routers leading to said host computer; said path comprising all routers in said network via which said packets are routed to said computer.

US7523497 B2 Claim 7	Darktrace
classifying data packets received at said host computer into wanted data packets and unwanted data packets by path;	<p>Supervised learning works by using previously-classified data, from which <u>the machine learns the classification system</u>. For scenarios where behaviors are well understood and classifications are easy to determine, the output of such systems can be highly accurate.</p> <p>For example, state-of-the-art image classification systems are outperforming humans in some cases. Indeed, what makes supervised machine learning so powerful is its ability to learn to deal with the errors and noise of the real world, through a statistical approach.</p> <p>Thus, supervised machine learning systems are best equipped to give you an explicit answer based on prior knowledge. For example, we can feed a system with lots of examples of known ransomware and it will learn the common indicators of that malware and be able to detect similar attacks in the future. However, overfitting is a common problem in supervised machine learning, where model parameters are too finely tuned to the training data.</p> <p>Instead of learning the essence of a category, the machine learns a particular example – for example, a machine may learn to recognize a German Shepherd, but fail to understand ‘dogs’ as a category, when distinguishing between ‘dogs’ and ‘cats,’ despite recognizing the features that make that German Shepherd pertain to the group.</p> <p><https://www.darktrace.com/en/resources/wp-machine-learning.pdf></p> <p>The reference describes classifying data packets received at said host computer into wanted data packets and unwanted data packets by path.</p>

US7523497 B2 Claim 7	Darktrace
associating a maximum acceptable processing rate with each class of data packet received at said host computer; and	<p>Detect</p> <ul style="list-style-type: none"> ○ <u>With self-learning AI, the Darktrace Immune System can detect the sophisticated and novel threats that policy-based controls simply can't.</u> <p>Respond</p> <ul style="list-style-type: none"> ○ Darktrace Antigena is the world's first Autonomous Response technology that can interrupt attacks on your behalf, at machine speed and with surgical precision. <p>Investigate</p> <ul style="list-style-type: none"> ○ Combining human security expertise with AI for the first time, Darktrace's Cyber AI Analyst automatically investigates every threat and reports on the full scope of incidents – reducing triage time by up to 92%. <p><https://www.darktrace.com/it/resources/ds-microsoft-azure.pdf> The reference describes associating a maximum acceptable processing rate with each class of data packet received at said host computer.</p>

US7523497 B2 Claim 7	Darktrace
allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.	<p>Detect</p> <ul style="list-style-type: none"> ○ With self-learning AI, the Darktrace Immune System can detect the sophisticated and novel threats that policy-based controls simply can't. <p>Respond</p> <ul style="list-style-type: none"> ○ Darktrace Antigena is the world's first <u>Autonomous Response technology that can interrupt attacks</u> on your behalf, at machine speed and with surgical precision. <p>Investigate</p> <ul style="list-style-type: none"> ○ Combining human security expertise with AI for the first time, Darktrace's Cyber AI Analyst automatically investigates every threat and reports on the full scope of incidents – reducing triage time by up to 92%. <hr/> <p>https://www.darktrace.com/it/resources/ds-microsoft-azure.pdf The reference describes allocating a processing rate less than or equal to said maximum acceptable processing rate for unwanted data packets.</p>

These allegations of infringement are preliminary and are therefore subject to change.

15. DARKTRACE has and continues to induce infringement. DARKTRACE has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., DDOS protection systems) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the ‘497 patent, literally or under the doctrine of equivalents. Moreover, DARKTRACE has known of the ‘497 patent and the technology underlying it from at least the filing date of the lawsuit.¹ For clarity, direct infringement is previously alleged in this complaint.

16. DARKTRACE has and continues to contributorily infringe. DARKTRACE has actively encouraged or instructed others (e.g., its customers and/or the customers of its related companies), and continues to do so, on how to use its products and services (e.g., DDOS protection systems) and related services that provide question and answer services across the Internet such as to cause infringement of one or more of claims 1–18 of the ‘497 patent, literally or under the doctrine of equivalents. Further, there are no substantial noninfringing uses for Defendant’s products and services. Moreover, DARKTRACE has known of the ‘497 patent and the technology underlying it from at least the filing date of the lawsuit.² For clarity, direct infringement is previously alleged in this complaint.

17. DARKTRACE has caused and will continue to cause PacSec3 damage by direct and indirect infringement of (including inducing infringement of) the claims of the ‘497 patent.

IV. JURY DEMAND

PacSec3 hereby requests a trial by jury on issues so triable by right.

V. PRAYER FOR RELIEF

¹ Plaintiff reserves the right to amend if discovery reveals an earlier date of knowledge.

² Plaintiff reserves the right to amend if discovery reveals an earlier date of knowledge.

WHEREFORE, PacSec3 prays for relief as follows:

- a. enter judgment that Defendant has infringed the claims of the '190 patent, the '564 patent and the '497 patent through selling, offering for sale, manufacturing, and inducing others to infringe by using and instructing to use DDOS protection systems;
- b. award PacSec3 damages in an amount sufficient to compensate it for Defendant's infringement of the Patent-in-Suit in an amount no less than a reasonable royalty or lost profits, together with pre-judgment and post-judgment interest and costs under 35 U.S.C. § 284;
- c. award PacSec3 an accounting for acts of infringement not presented at trial and an award by the Court of additional damage for any such acts of infringement;
- d. declare this case to be "exceptional" under 35 U.S.C. § 285 and award PacSec3 its attorneys' fees, expenses, and costs incurred in this action;
- e. declare Defendant's infringement to be willful and treble the damages, including attorneys' fees, expenses, and costs incurred in this action and an increase in the damage award pursuant to 35 U.S.C. § 284;
- f. a decree addressing future infringement that either (i) awards a permanent injunction enjoining Defendant and its agents, servants, employees, affiliates, divisions, and subsidiaries, and those in association with Defendant from infringing the claims of the Patent-in-Suit, or (ii) awards damages for future infringement in lieu of an injunction in an amount consistent with the fact that for future infringement the Defendant will be an adjudicated infringer of a valid patent, and trebles that amount in view of the fact that the future infringement will be willful as a matter of law; and
- g. award PacSec3 such other and further relief as this Court deems just and proper.

Respectfully submitted,

Ramey & Schwaller, LLP

/s/William P. Ramey

William P. Ramey, III

Texas Bar No. 24027643

5020 Montrose Blvd., Suite 800

Houston, Texas 77006

(713) 426-3923 (telephone)

(832) 900-4941 (fax)

wramey@rameyfirm.com

Attorneys for PacSec3, LLC